TABLE OF y^x (mod 13) OF PRIME 13

y^x	1	2	3	4	5	6	7	8	9	10	11	12	ORDER
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	3	6	12	11	9	5	10	7	1	12
3	3	9	1	3	9	1	3	9	1	3	9	1	3
4	4	3	12	9	10	1	4	3	12	9	10	1	6
5	5	12	8	1	5	12	8	1	5	12	8	1	4
6	6	10	8	9	2	12	7	3	5	4	11	1	12
7	7	10	5	9	11	12	6	3	8	4	2	1	12
8	8	12	5	1	8	12	5	1	8	12	5	1	4
9	9	3	1	9	3	1	9	3	1	9	3	1	3
10	10	9	12	3	4	1	10	9	12	3	4	1	6
11	11	4	5	3	7	12	2	9	8	10	6	1	12
12	12	1	12	1	12	1	12	1	12	1	12	1	2

FIG. 1

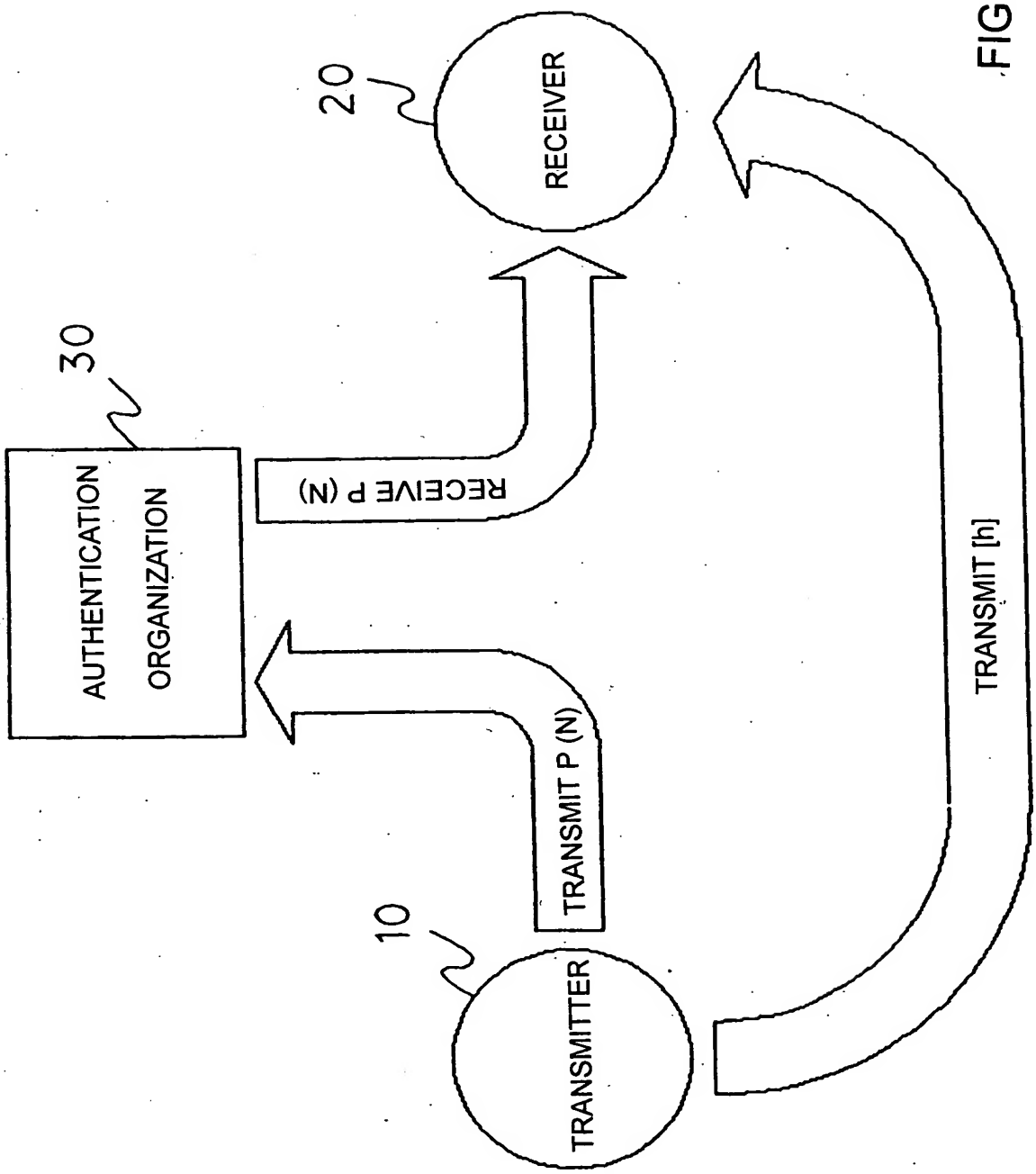

20
RECEIVER
30
AUTHENTICATION ORGANIZATION
RECEIVE P (N)
TRANSMIT P (N)
10
TRANSMITTER
TRANSMIT [h]

FIG. 2

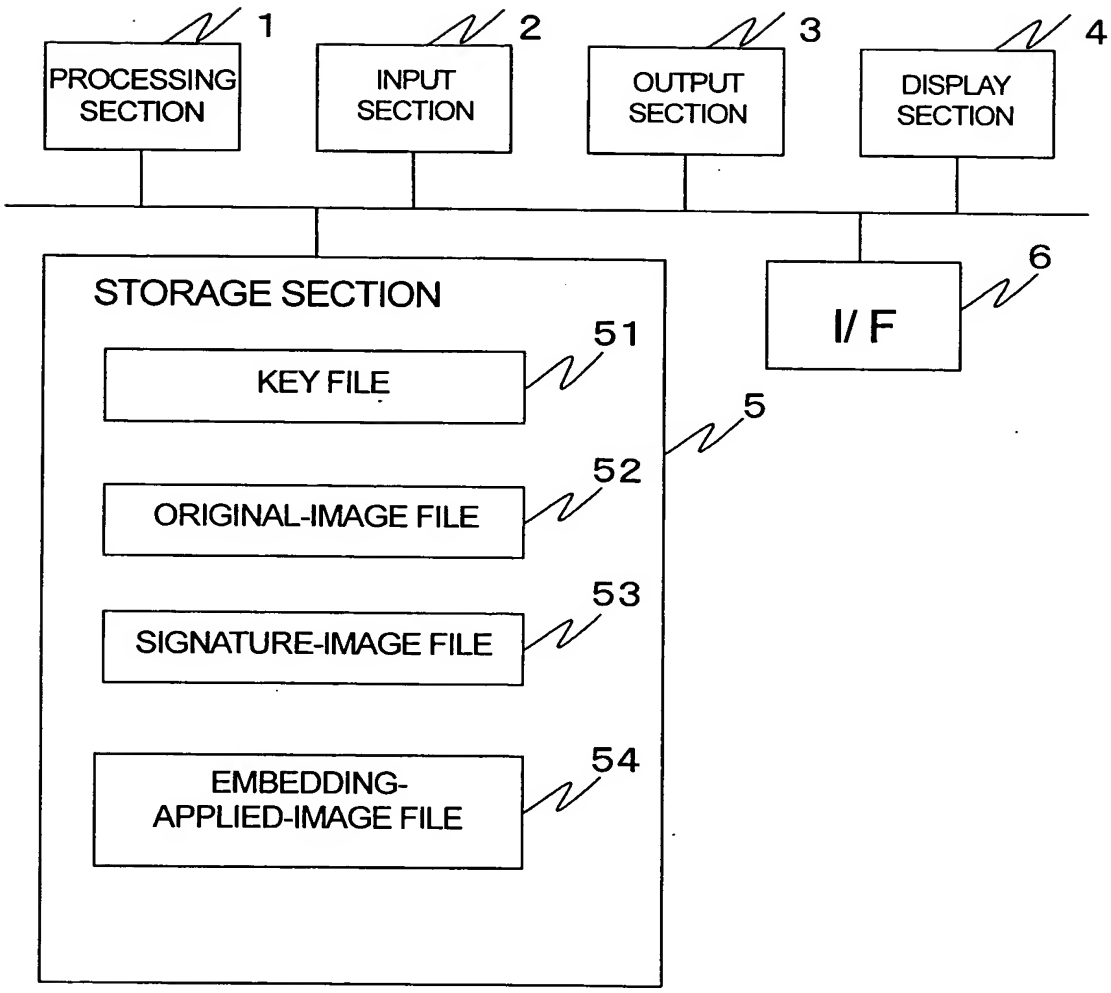

1
PROCESSING SECTION
2
INPUT SECTION
3
OUTPUT SECTION
4
DISPLAY SECTION
STORAGE SECTION
51
KEY FILE
52
ORIGINAL-IMAGE FILE
53
SIGNATURE-IMAGE FILE
54
EMBEDDING-APPLIED-IMAGE FILE
5
I/F
6

FIG. 3

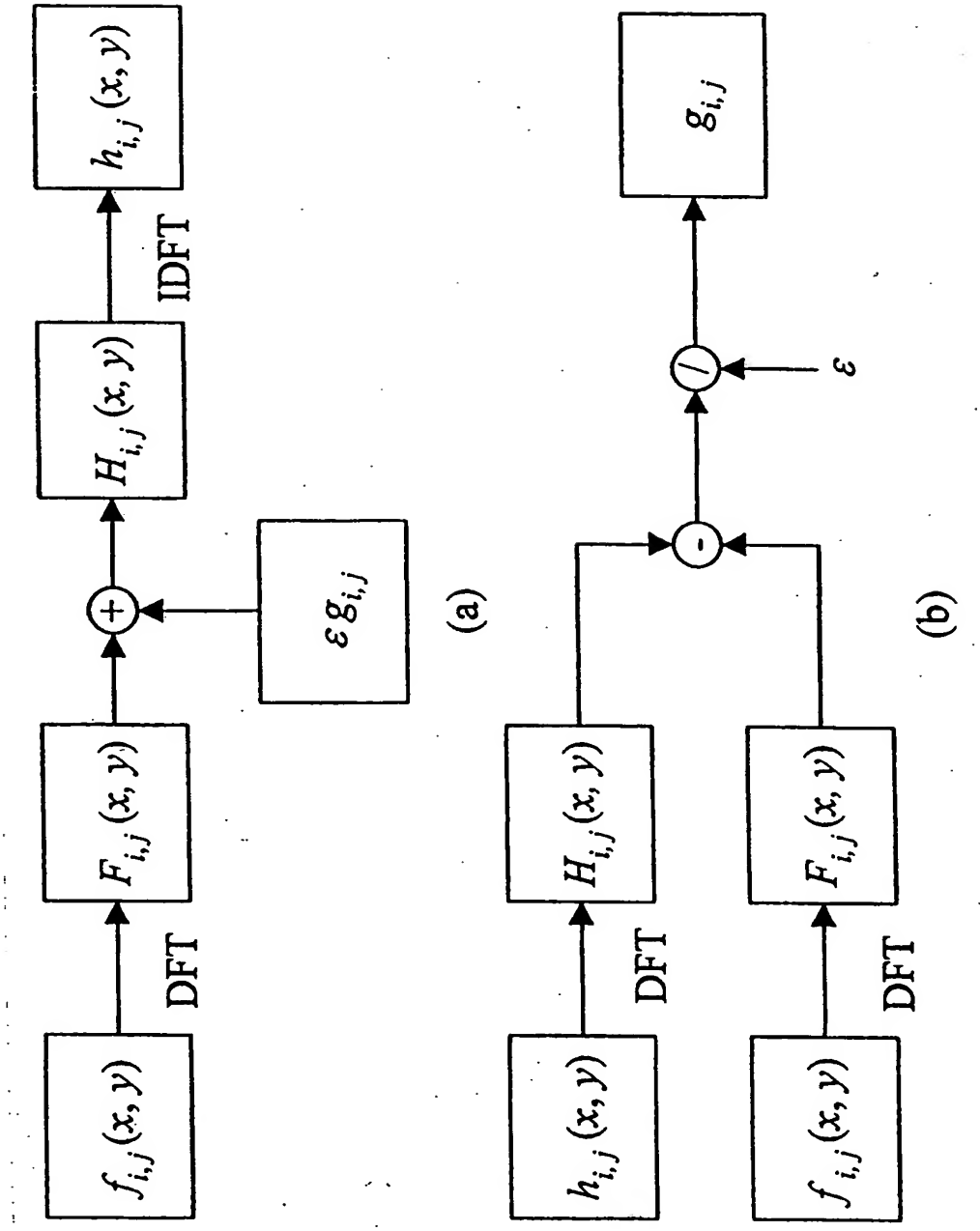

$f_{i,j}(x,y)$
DFT
$F_{i,j}(x,y)$
$\varepsilon g_{i,j}$
$H_{i,j}(x,y)$
IDFT
$h_{i,j}(x,y)$
(a)
$h_{i,j}(x,y)$
DFT
$H_{i,j}(x,y)$
$f_{i,j}(x,y)$
DFT
$F_{i,j}(x,y)$
ε
$g_{i,j}$
(b)

FIG. 4

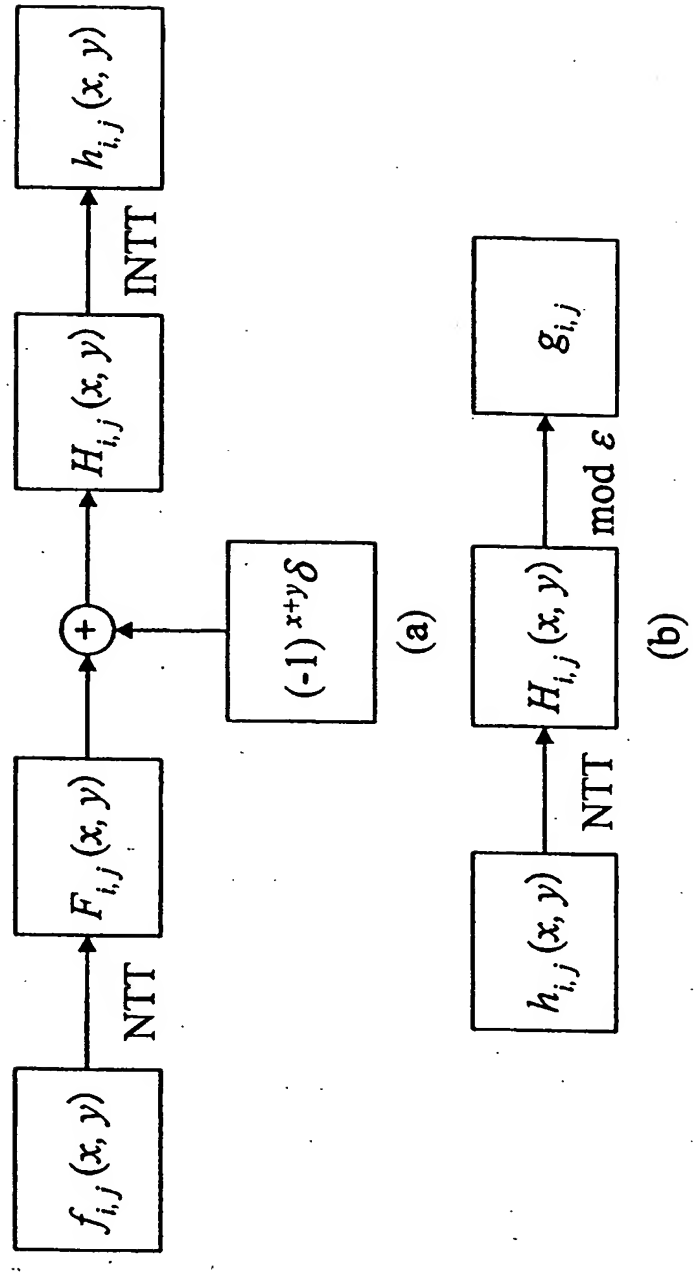

$f_{i,j}(x, y)$
NTT
$F_{i,j}(x, y)$
+
$(-1)^{x+y}\delta$
(a)
$H_{i,j}(x, y)$
INTT
$h_{i,j}(x, y)$
$h_{i,j}(x, y)$
NTT
$H_{i,j}(x, y)$
mod ε
$g_{i,j}$
(b)

FIG. 5

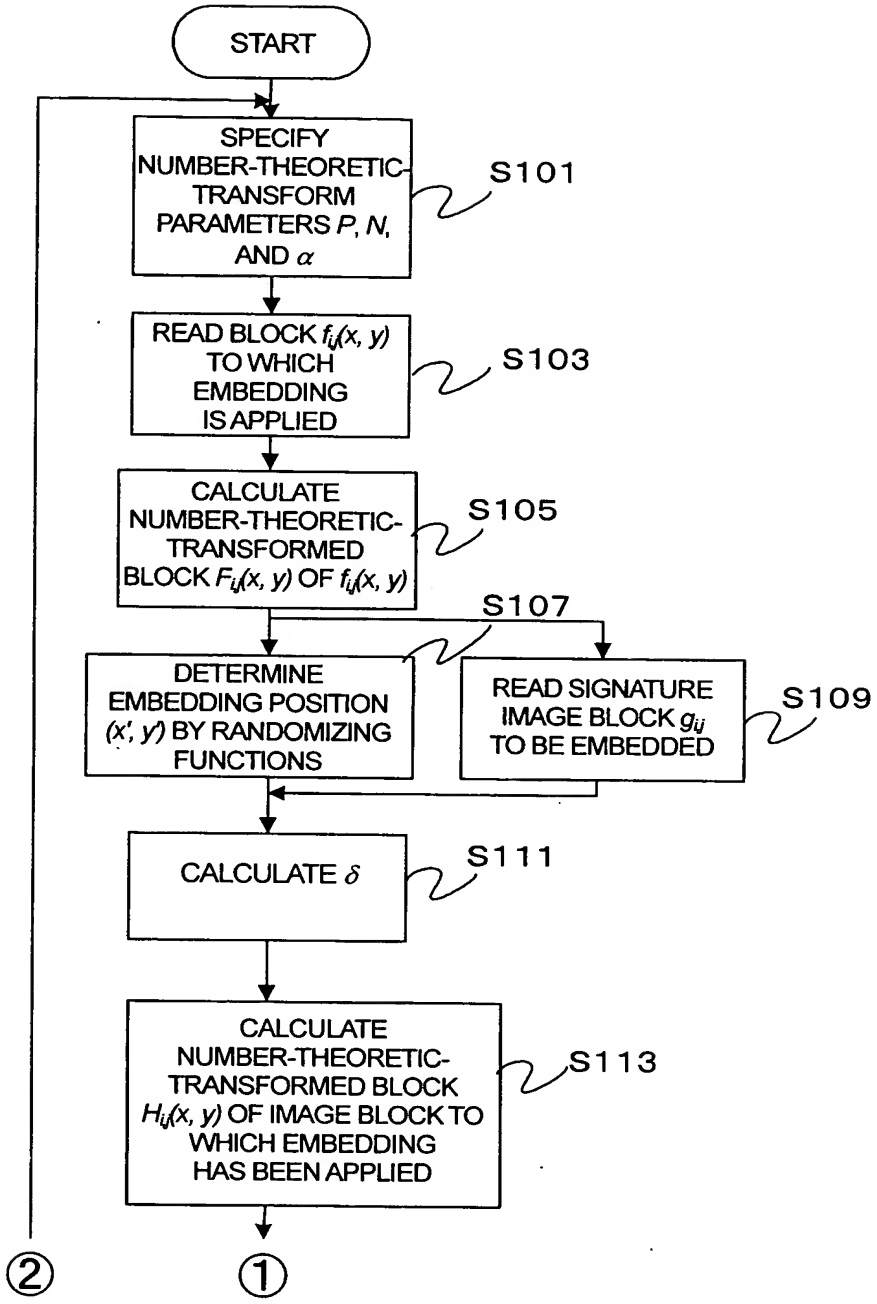

START
SPECIFY NUMBER-THEORETIC-TRANSFORM PARAMETERS P, N, AND α
S101
READ BLOCK $f_{ij}(x, y)$ TO WHICH EMBEDDING IS APPLIED
S103
CALCULATE NUMBER-THEORETIC-TRANSFORMED BLOCK $F_{ij}(x, y)$ OF $f_{ij}(x, y)$
S105
S107
DETERMINE EMBEDDING POSITION (x', y') BY RANDOMIZING FUNCTIONS
READ SIGNATURE IMAGE BLOCK g_{ij} TO BE EMBEDDED
S109
CALCULATE δ
S111
CALCULATE NUMBER-THEORETIC-TRANSFORMED BLOCK $H_{ij}(x, y)$ OF IMAGE BLOCK TO WHICH EMBEDDING HAS BEEN APPLIED
S113
②
①

FIG. 6

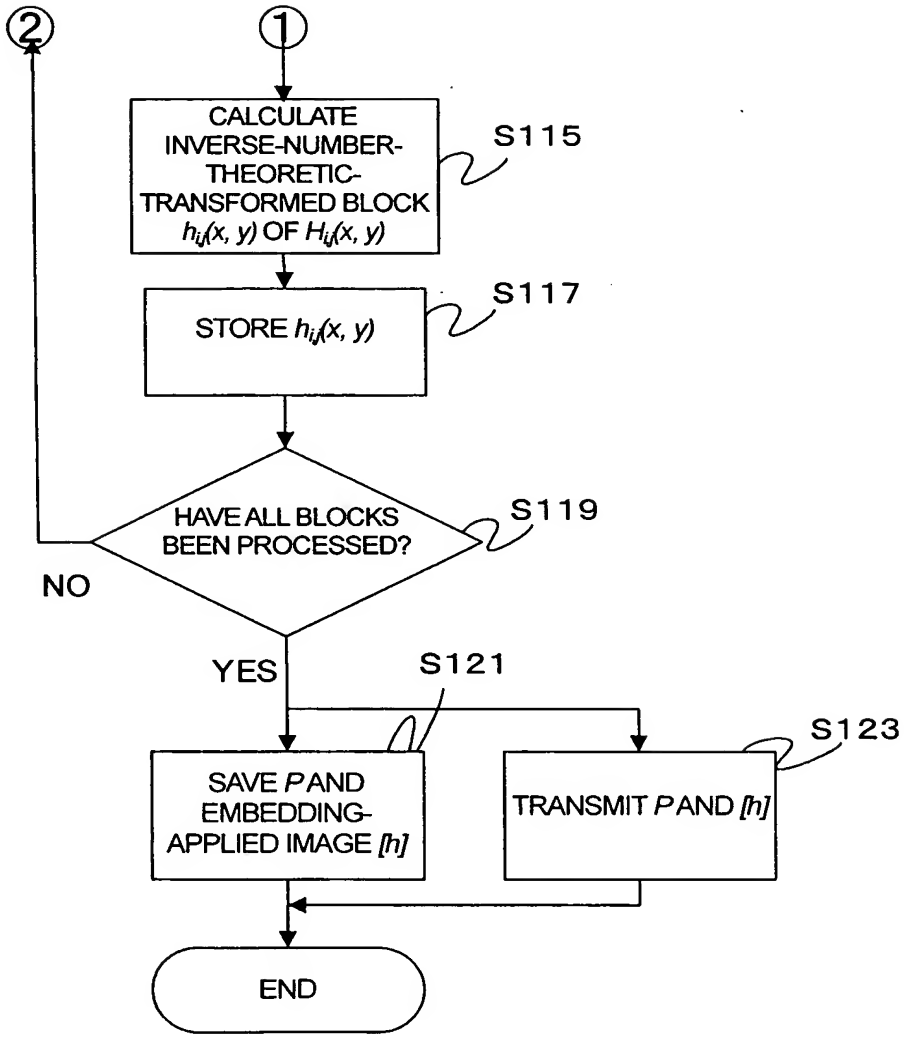

②
①
CALCULATE INVERSE-NUMBER-THEORETIC-TRANSFORMED BLOCK $h_{ij}(x, y)$ OF $H_{ij}(x, y)$
S115
STORE $h_{ij}(x, y)$
S117
HAVE ALL BLOCKS BEEN PROCESSED?
S119
NO
YES
S121
S123
SAVE P AND EMBEDDING-APPLIED IMAGE [h]
TRANSMIT P AND [h]
END

FIG. 7

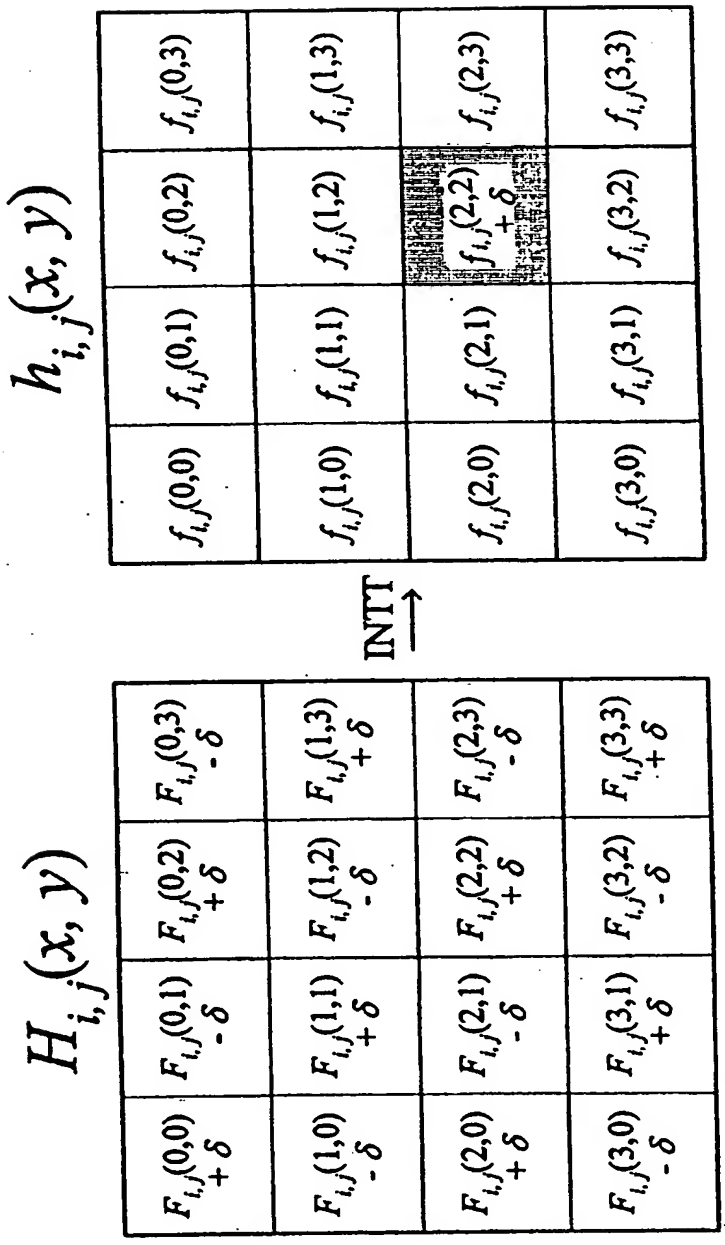

$H_{i,j}(x, y)$
$F_{i,j}(0,0) + \delta$
$F_{i,j}(0,1) - \delta$
$F_{i,j}(0,2) + \delta$
$F_{i,j}(0,3) - \delta$
$F_{i,j}(1,0) - \delta$
$F_{i,j}(1,1) + \delta$
$F_{i,j}(1,2) - \delta$
$F_{i,j}(1,3) + \delta$
$F_{i,j}(2,0) + \delta$
$F_{i,j}(2,1) - \delta$
$F_{i,j}(2,2) + \delta$
$F_{i,j}(2,3) - \delta$
$F_{i,j}(3,0) - \delta$
$F_{i,j}(3,1) + \delta$
$F_{i,j}(3,2) - \delta$
$F_{i,j}(3,3) + \delta$
INTT
$h_{i,j}(x, y)$
$f_{i,j}(0,0)$
$f_{i,j}(0,1)$
$f_{i,j}(0,2)$
$f_{i,j}(0,3)$
$f_{i,j}(1,0)$
$f_{i,j}(1,1)$
$f_{i,j}(1,2)$
$f_{i,j}(1,3)$
$f_{i,j}(2,0)$
$f_{i,j}(2,1)$
$f_{i,j}(2,2) + \delta$
$f_{i,j}(2,3)$
$f_{i,j}(3,0)$
$f_{i,j}(3,1)$
$f_{i,j}(3,2)$
$f_{i,j}(3,3)$

FIG. 8

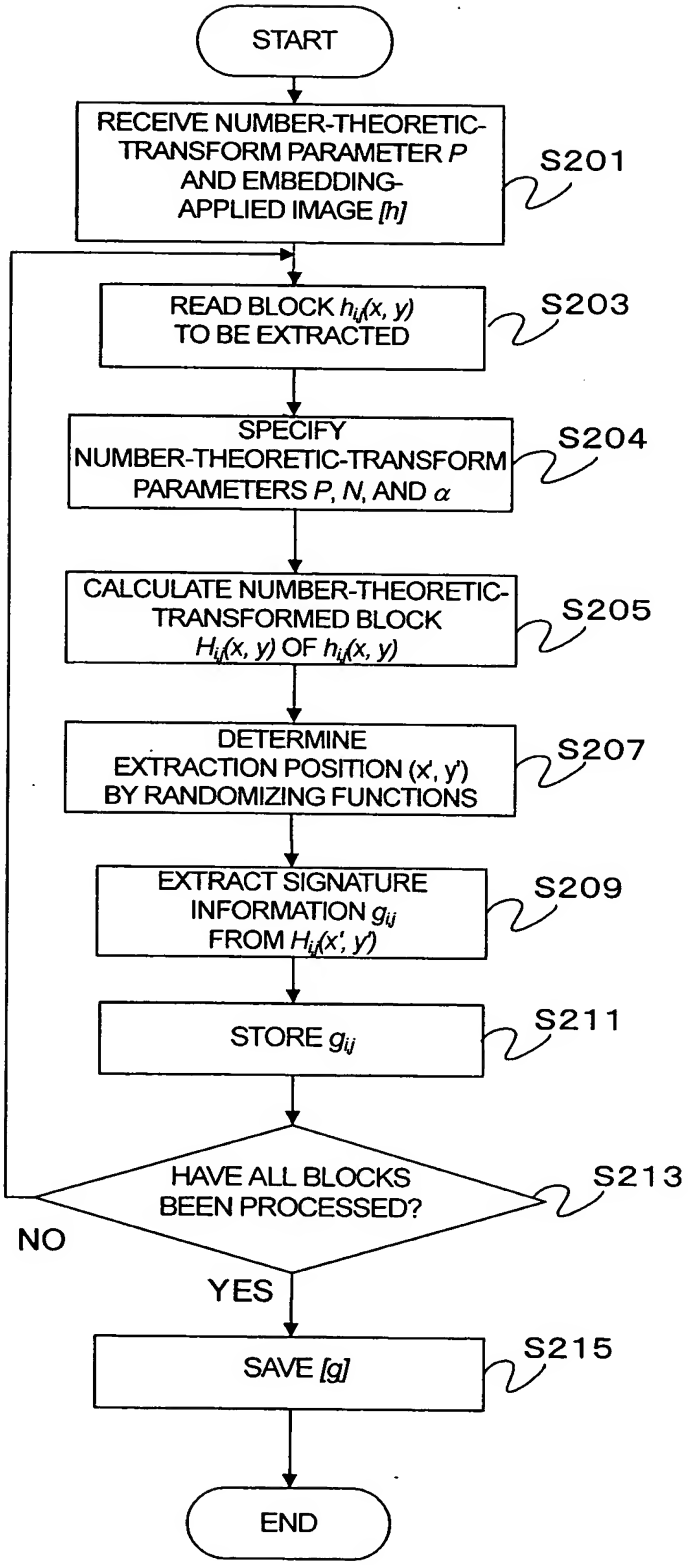
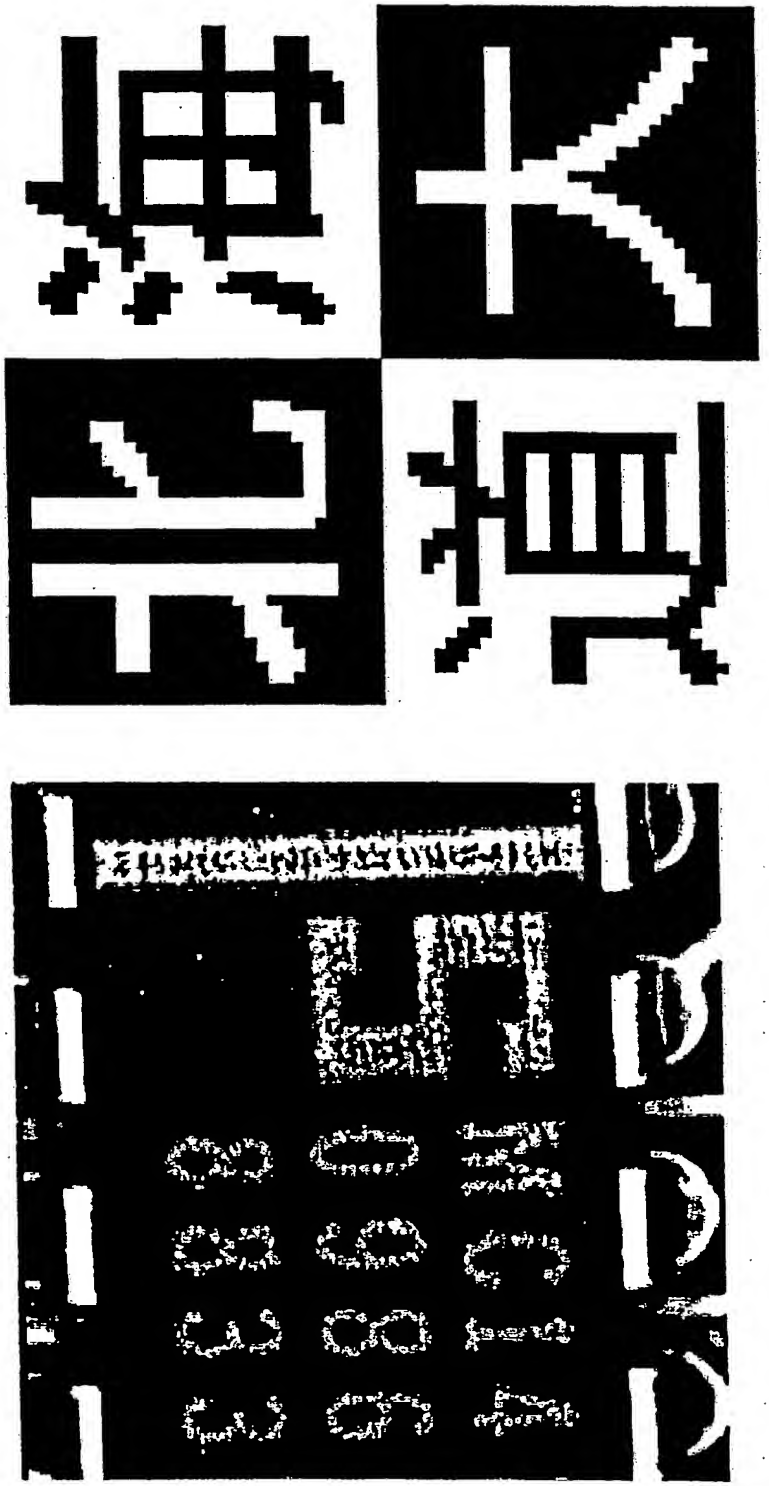

START
RECEIVE NUMBER-THEORETIC-TRANSFORM PARAMETER P AND EMBEDDING-APPLIED IMAGE [h]
S201
READ BLOCK $h_{ij}(x, y)$ TO BE EXTRACTED
S203
SPECIFY NUMBER-THEORETIC-TRANSFORM PARAMETERS P, N, AND α
S204
CALCULATE NUMBER-THEORETIC-TRANSFORMED BLOCK $H_{ij}(x, y)$ OF $h_{ij}(x, y)$
S205
DETERMINE EXTRACTION POSITION (x', y') BY RANDOMIZING FUNCTIONS
S207
EXTRACT SIGNATURE INFORMATION g_{ij} FROM $H_{ij}(x', y')$
S209
STORE g_{ij}
S211
HAVE ALL BLOCKS BEEN PROCESSED?
S213
NO
YES
SAVE [g]
S215
END

FIG. 9

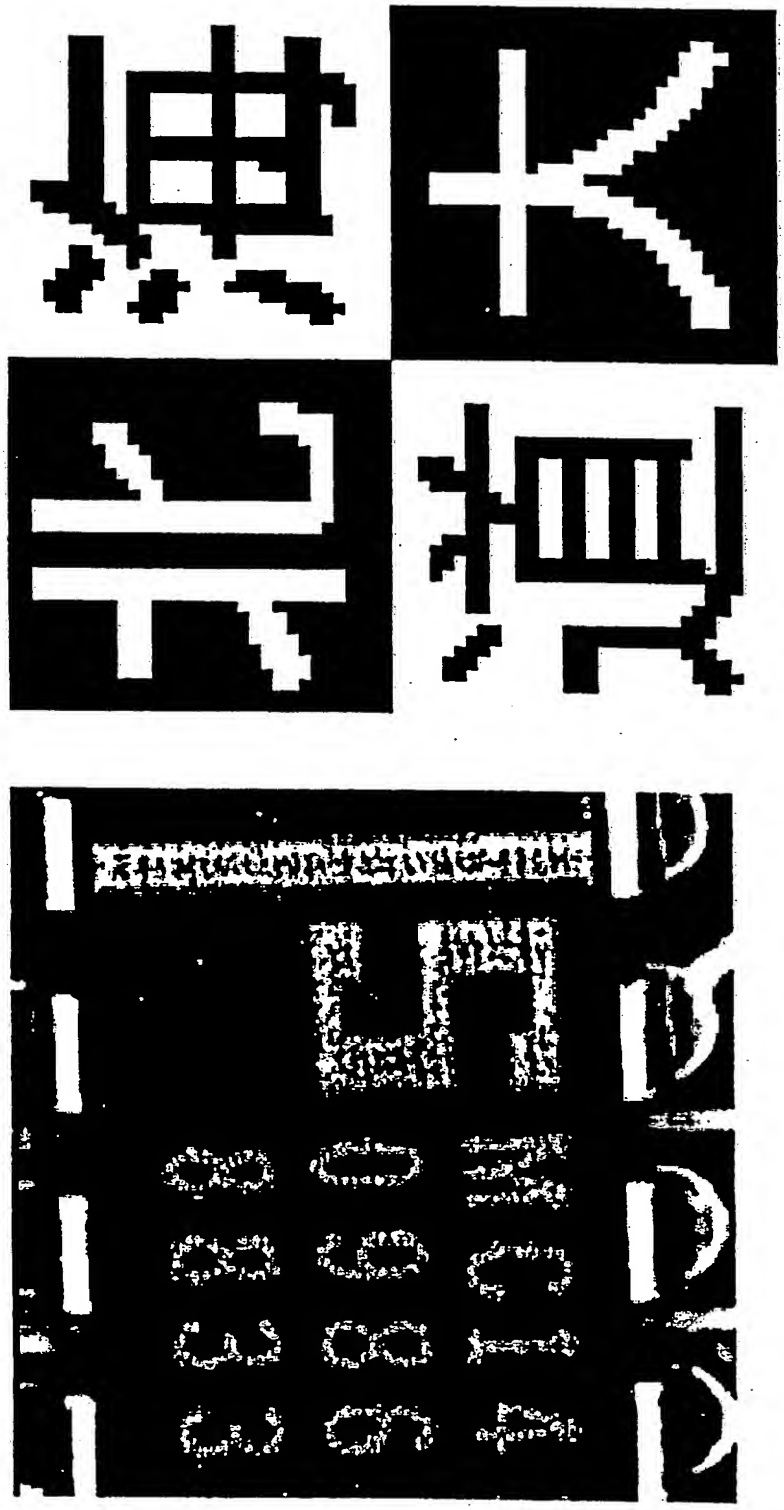


(b)

(a)

FIG. 10

Best Available Copy



(b)

(a)

FIG. 11

Best Available Copy

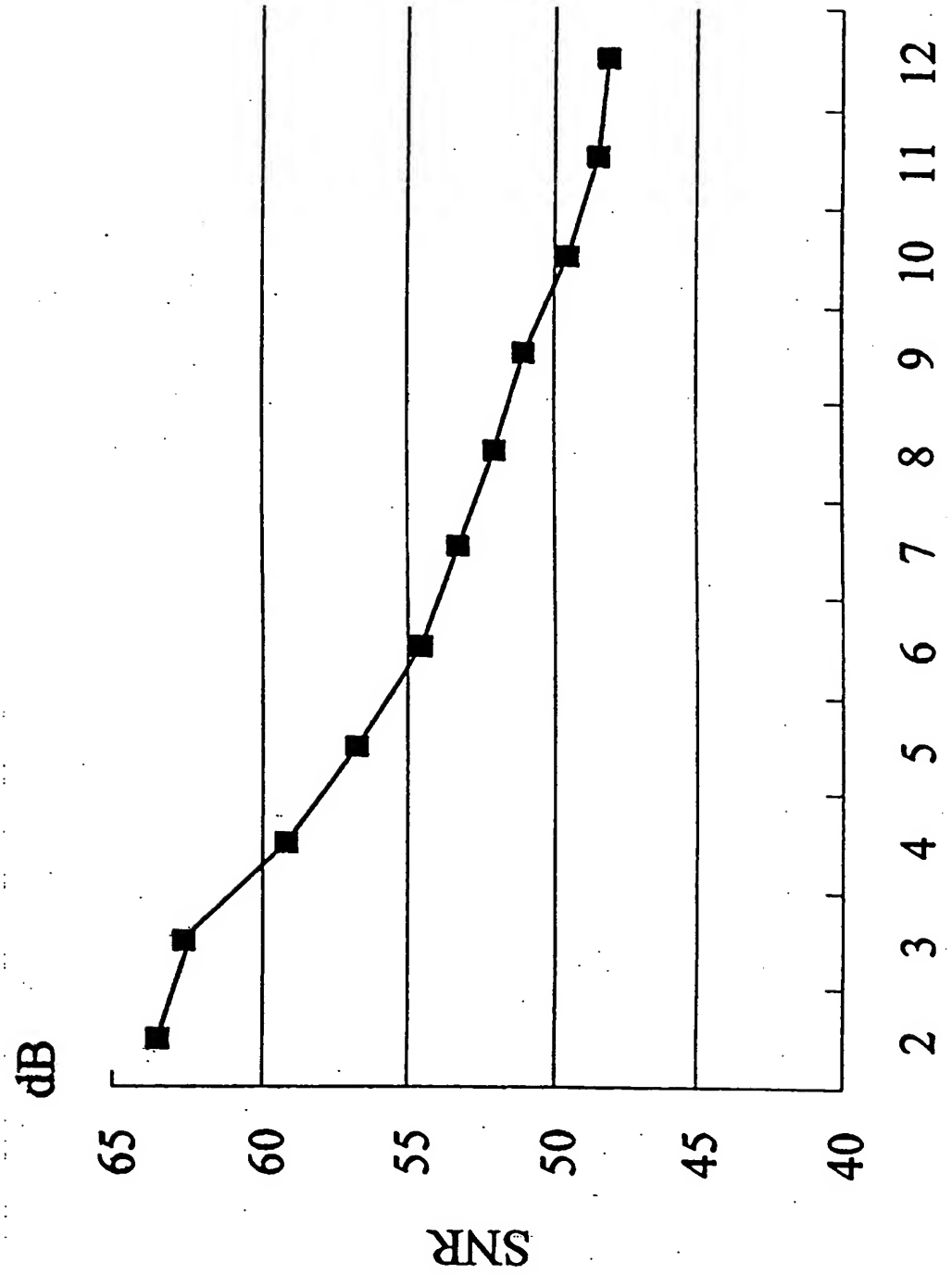


FIG. 12

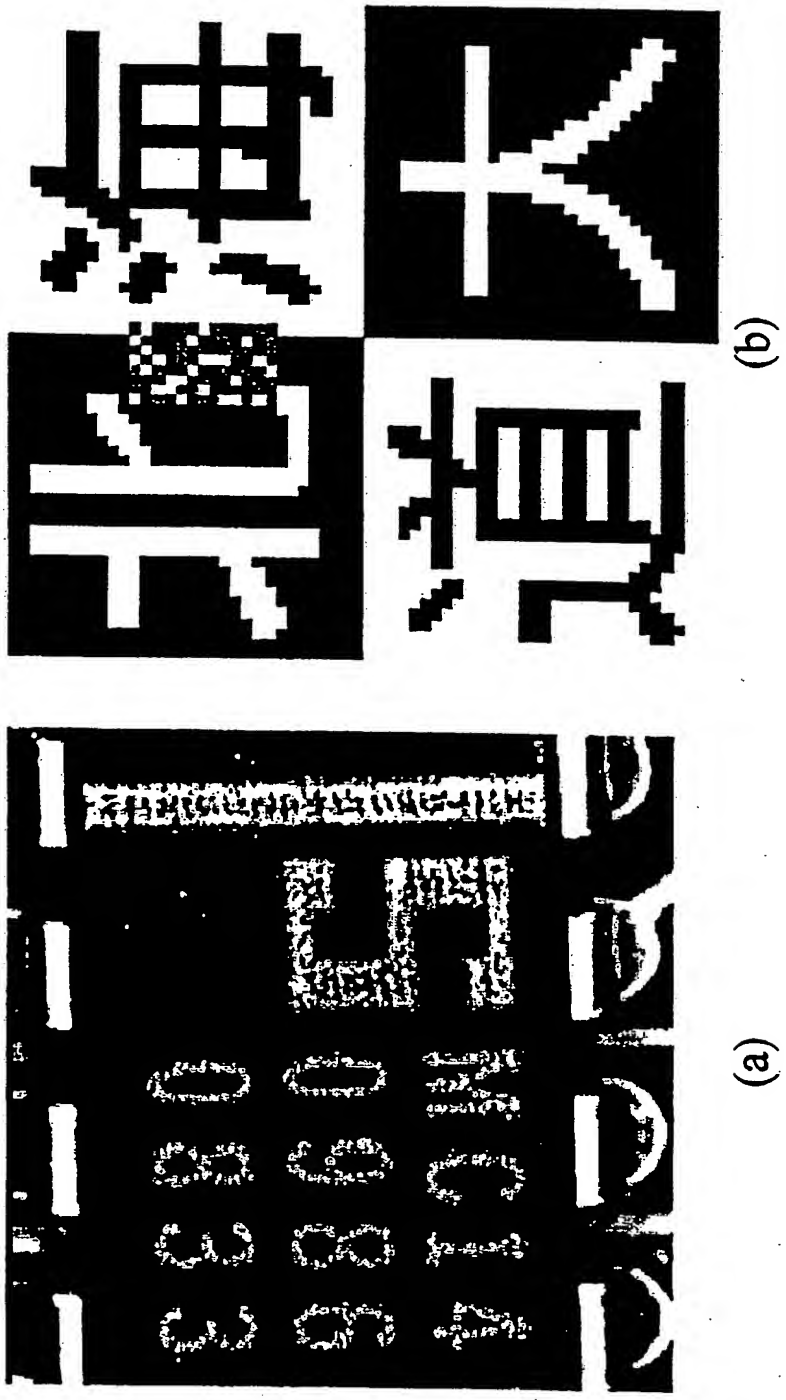


FIG. 13

Best Available Copy